RECEIVED
CENTRAL FAX CENTER

SEP 07 2006

In re Patent Application of
MACCHETTI ET AL.
Serial No. **09/974,705**
Filed: **OCTOBER 10, 2001**

REMARKS

Applicants thank the Examiner for the careful and thorough examination of the present application. By this amendment, Claims 21, 31 and 44 have been amended to further clarify the present invention, and Claim 25 has been amended to eliminate minor informalities contained therein. Claims 21-47 remain pending in the application. Favorable reconsideration is respectfully requested.

I. The Claimed Invention

Independent Claim 31, for example, is directed to a device for converting data between an unencrypted format and an encrypted format. The device comprises a register for storing the data in the form of bit words, and a circuit. The circuit is for performing a plurality of transformation rounds, with each transformation round comprising applying at least one transformation to a two-dimensional array of rows and columns of bit words defining a state array. Furthermore, each of the rows is exchanged with a respective column of the state array to form a transposed state array for at least one of the transformation rounds so that at least one transformation is applied to the transposed state array (as described on page 8, lines 2-9 of the specification and explicitly shown in FIG. 5 of the drawings). Independent Claim 21 is a method counterpart to Claim 31 and recites similar recitations. Independent Claim 44 is similar to Claim 31, but further recites that each transformation round also comprises applying at least one round key to the state array in at least one of the transformation rounds.

In re Patent Application of
MACCHETTI ET AL.
Serial No. **09/974,705**
Filed: **OCTOBER 10, 2001**

II. The Claims are Patentable

Claims 21-47 were rejected as allegedly failing to comply with the written description requirement. The Examiner asserts that the specification fails to disclose "transposing each of the rows and columns of the state array to form a transposed state array" as claimed.

As the Examiner is aware, to satisfy the written description requirement, a patent specification must describe the claimed invention in sufficient detail that one skilled in the art can reasonably conclude that the inventor had possession of the claimed invention. There is no exact words requirement, as claim limitations can be supported in the specification through express, implicit, or inherent disclosure. The fundamental factual inquiry is whether the specification conveys with reasonable clarity to those skilled in the art that Applicant was in possession of the invention as now claimed.

A careful review of the specification and drawings reveals that "transposing each of the rows and columns of the state array to form a transposed state array" is clearly disclosed e.g. on page 8, lines 2-9 of the specification and explicitly shown in FIG. 5 of the drawings. Furthermore, the claims have been amended to recite that "each of the rows is exchanged with a respective column of the state array to form a transposed state array" to further clarify the present invention. Accordingly, Applicants believe that the claims comply with the requirements of 35 U.S.C. §112, first paragraph.

The Examiner again rejected independent Claims 21, 31, and 44 as being unpatentable over the Ohkuma et al. patent

publication for the reasons set forth on pages 5-9 of the Office Action. Applicants contend that independent Claims 21, 31 and 44, and their respective dependent claims, clearly define over the cited reference, and in view of the following remarks, favorable reconsideration of the rejection under 35 U.S.C. §103 is requested.

Each of the amended independent claims now includes exchanging each of the rows with a respective column of the state array to form a transposed state array for at least one of the transformation rounds so that at least one transformation is applied to the transposed state array. It is this combinations of features which is not fairly taught or suggested in the cited reference and which patentably defines over the cited reference.

Although Applicants believe that the Examiner has continued to mischaracterize the actual teachings of the reference with respect to the higher level MDS (Maximum Distance Separable) matrix, the claims have been amended to further clarify the features of the invention and advance prosecution of the application. Specifically, the Examiner incorrectly contends (sections 2.1 and 5.2 of the Office Action) that in the Ohkuma et al. patent publication, "transposing is performed by substituting rows and substituting columns to obtain a transposed MDS matrix (state array) that meets the recitation of transposing each row and column of the state array to form a transposed state array".

As support for this contention, the Examiner points to paragraphs [0261]-[0271] of the Ohkuma et al. patent publication. Yet paragraph [0268] merely states that a matrix may be obtained by substituting rows, substituting columns,

and arbitrarily transposing in an arbitrary MDS matrix. There is nothing in any of the cited paragraphs specifically relied upon by the Examiner that discloses or suggests transposing each of the rows and columns of a state array. The Examiner is relying upon the Ohkuma et al. reference merely for the use of the term "transposing" included therein.

So, Applicants have now amended the independent claims to recite exchanging each of the rows with a respective column of the state array to form a transposed state array. Accordingly, the phrase "arbitrarily transposing" in the reference cannot be fairly interpreted to meet the features of the invention as claimed. In other words, in Ohkuma et al., there is clearly no exchanging of each of the rows with a respective column of the state array to form a transposed state array.

Thus, there is simply no teaching or suggestion in the cited reference to provide the combination of features as claimed. Accordingly, for at least the reasons given above, Applicants maintain that the cited reference does not disclose or fairly suggests the invention as set forth in Claims 21, 31 and 44. Furthermore, no proper modification of the teachings of this reference could result in the invention as claimed. Thus, the rejection under 35 U.S.C. §103(a) should be withdrawn.

It is submitted that the independent claims are patentable over the prior art. In view of the patentability of the independent claims, it is submitted that their dependent claims, which recite yet further distinguishing features are also patentable over the cited references for at

In re Patent Application of
MACCHETTI ET AL.
Serial No. **09/974,705**
Filed: **OCTOBER 10, 2001**

least the reasons set forth above. Accordingly, these dependent claims require no further discussion herein.

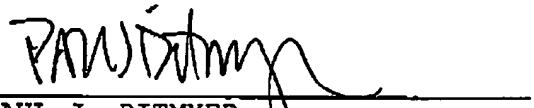
III. Request for Interview

After reviewing this amendment and considering the arguments, the Examiner is respectfully requested to contact the Applicants' representative at the telephone number listed below to schedule a time for an interview to discuss any remaining issues.

IV. Conclusion

In view of the foregoing remarks, it is respectfully submitted that the present application is in condition for allowance. An early notice thereof is earnestly solicited.

Respectfully submitted,



PAUL J. DITMYER
Reg. No. 40,455
Allen, Dyer, Doppelt, Milbrath
& Gilchrist, P.A.
255 S. Orange Avenue, Suite 1401
Post Office Box 3791
Orlando, Florida 32802
407-841-2330
407-841-2343 fax
Attorney for Applicants